

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-203237

(43)Date of publication of application : 30.07.1999

(51)Int.Cl.

G06F 13/36
G06F 13/38
G06F 15/78
G06K 19/073

(21)Application number : 10-006509

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 16.01.1998

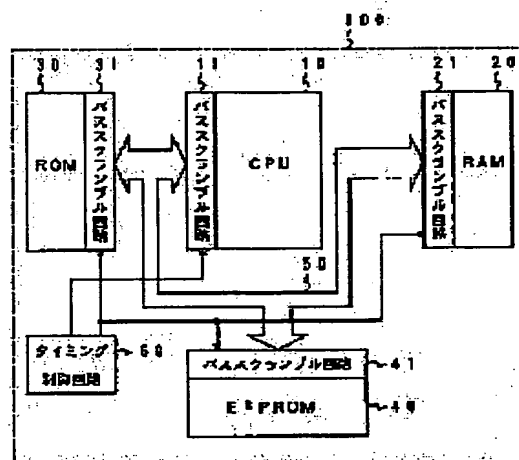
(72)Inventor : HASEBE SHINICHI

(54) SEMICONDUCTOR INTEGRATED CIRCUIT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a new security system an IC internal part of which can not easily be analyzed.

SOLUTION: Order of an address and data outputted from a CPU 10 are changed regularly or in a random cycle by a bus scramble circuit 11. Thus, the address and the data outputted to each of plural bus lines 50 change hour to hour and cannot specify the meaning (kind) of the data given to a specified bus line. The address and the data of the bus line 50 have their order returned to the original order by the bus scramble circuits 21, 31 and 41 before they are inputted to memories 20, 30 and 40. A timing control circuit 60 changes the order of the address and the data and decides a cycle in which the order is returned to the original one.



LEGAL STATUS

[Date of request for examination] 15.06.2001

[Date of sending the examiner's decision of rejection] 03.06.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-203237

(43) 公開日 平成11年(1999) 7月30日

(51) IntCl.⁶

識別記号

F I

G 0 6 F 13/36

3 2 0

G 0 6 F 13/36

3 2 0 Z

13/38

3 3 0

13/38

3 3 0 Z

15/78

5 1 0

15/78

5 1 0 G

G 0 6 K 19/073

G 0 6 K 19/00

P

審査請求 未請求 請求項の数 5 O L (全 5 頁)

(21) 出願番号

特願平10-6509

(22) 出願日

平成10年(1998) 1月16日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 長谷部 信一

神奈川県川崎市幸区堀川町580番1号 株

式会社東芝半導体システム技術センター内

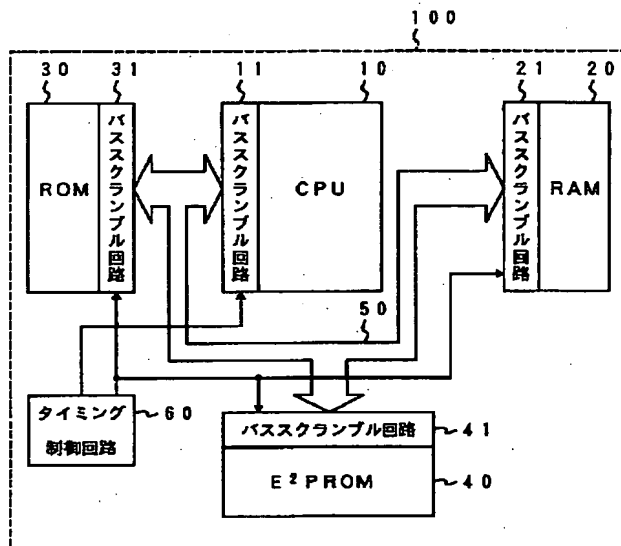
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 半導体集積回路

(57) 【要約】

【課題】 IC内部を解析されない新規なセキュリティシステムを提供する。

【解決手段】 CPU 10から出力されるアドレス及びデータの順序は、バススクランブル回路 11により、定期的又はランダムな周期で変えられる。このため、複数本のバスライン 50の各々に出力されるアドレス及びデータは、時々刻々と変化し、所定のバスラインに与えられるデータの意味(種類)を特定することはできない。バスライン 50のアドレス及びデータは、メモリ 20、30、40に入力される前に、バススクランブル回路 21、31、41により元の順序に戻される。タイミング制御回路 60は、アドレス及びデータの順序を変え、元に戻す周期を決定する。



【特許請求の範囲】

【請求項1】 複数ビットの信号を送信する第1ブロックと、前記複数ビットの信号を受信する第2ブロックと、前記複数ビットの信号を前記第1ブロックから前記第2ブロックへ転送する複数本のバスラインと、前記第1ブロックから出力される複数ビットの信号の順序を変えて前記複数本のバスラインに導く第1バススクランブル回路と、前記複数本のバスラインの複数ビットの信号の順序を元に戻して前記第2ブロックに導く第2バススクランブル回路とを具備することを特徴とする半導体集積回路。

【請求項2】 請求項1記載の半導体集積回路において、さらに、前記第1ブロックから出力される複数ビットの信号の順序を定期的又はランダムな周期で変えるように前記第1バススクランブル回路を制御し、前記複数本のバスラインの複数ビットの信号の順序を定期的又はランダムな周期で元に戻すように前記第2バススクランブル回路を制御するタイミング制御回路を具備することを特徴とする半導体集積回路。

【請求項3】 前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第1ブロックから出力される複数ビットの信号のうちの所定の1ビットの値により決定することを特徴とする請求項2記載の半導体集積回路。

【請求項4】 前記第1ブロックは、CPUの機能を有し、前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第1ブロックから出力されるクロックの周期よりも長く設定されていることを特徴とする請求項2記載の半導体集積回路。

【請求項5】 前記第1ブロックは、CPUの機能を有し、前記第2ブロックは、メモリの機能を有し、前記複数ビットの信号は、前記メモリをアクセスするアドレス又は前記メモリに入力するデータを含んでいることを特徴とする請求項2記載の半導体集積回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、IC（半導体集積回路）の内部を悪意のあるアタッカーに解析されないように、アドレスバス及びデータバスに出力するアドレス及びデータの順序をランダムに変えるセキュリティシステムに関する。

【0002】

【従来の技術】従来、ICカードなどのセキュリティの必要のある製品においては、ICの内部を悪意のあるアタッカーに解析されないように、アドレスバス及びデータバスを物理的に混在させて、容易にICの内部を解析できないようにしていた。

【0003】しかし、このようなセキュリティシステムでは、ICの製造段階（配線工程）において、マスクの

パターンによりアドレスバス及びデータバスの配置（順序）が決定されてしまい、ICの製造後に、アドレスバス及びデータバスの配置をランダムに変えることができない。

【0004】このため、悪意のあるアタッカーがICの内部を繰り返し解析すると、最後には、アドレスバス及びデータバスの配置が判明してしまい、ICのセキュリティが十分に行われていなかった。

【0005】

【発明が解決しようとする課題】このように、従来は、悪意のあるアタッカーがICの内部を繰り返し解析すると、最後には、アドレスバス及びデータバスの配置が判明してしまい、ICのセキュリティが十分に行われないという欠点がある。

【0006】本発明は、上記欠点を解決すべくなされたもので、その目的は、悪意のあるアタッカーがICの内部を繰り返し解析しても、アドレス及びデータを特定できないような新規なセキュリティシステムを提供することである。

【0007】

【課題を解決するための手段】上記目的を達成するため、本発明の半導体集積回路は、複数ビットの信号を送信する第1ブロックと、前記複数ビットの信号を受信する第2ブロックと、前記複数ビットの信号を前記第1ブロックから前記第2ブロックへ転送する複数本のバスラインと、前記第1ブロックから出力される複数ビットの信号の順序を変えて前記複数本のバスラインに導く第1バススクランブル回路と、前記複数本のバスラインの複数ビットの信号の順序を元に戻して前記第2ブロックに導く第2バススクランブル回路とを備える。

【0008】本発明の半導体集積回路は、さらに、前記第1ブロックから出力される複数ビットの信号の順序を定期的又はランダムな周期で変えるように前記第1バススクランブル回路を制御し、前記複数本のバスラインの複数ビットの信号の順序を定期的又はランダムな周期で元に戻すように前記第2バススクランブル回路を制御するタイミング制御回路を備える。

【0009】前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第1ブロックから出力される複数ビットの信号のうちの所定の1ビットの値により決定する。

【0010】前記第1ブロックがCPUの機能を有している場合、前記複数ビットの信号の順序を変え、かつ、元に戻す周期は、前記第1ブロックから出力されるクロックの周期よりも長く設定される。

【0011】前記第1ブロックがCPUの機能を有し、前記第2ブロックがメモリの機能を有している場合、前記複数ビットの信号は、前記メモリをアクセスするアドレス又は前記メモリに入力するデータを含んでいる。

【0012】

【発明の実施の形態】以下、図面を参照しながら、本発明の半導体集積回路について詳細に説明する。図1は、本発明に関わるバススクランブル回路を有するIC（半導体集積回路）の内部構成の一例を示している。

【0013】IC100内は、複数のブロックから構成されており、例えば、複数のブロックには、CPU（central processing unit）10、RAM（random access memory）20、ROM（read only memory）30、E² PROM（electrically erasable programmable ROM）40などが含まれている。

【0014】各ブロック10、20、30、40のI/O部（データの入出力部）及びアドレスの入出力部には、これらに隣接する形でバススクランブル回路11、21、31、41が設けられている。また、各バススクランブル回路11、21、31、41を互いに接続するバスライン50が配置されている。バスライン50は、n（例えば、16）ビットのアドレスバス及びm（例えば、8）ビットのデータバスから構成されている。

【0015】タイミング制御回路60は、各ブロックに対応して設けられたバススクランブル回路の動作を制御する。タイミング制御回路60は、例えば、図3に示すようなフリップフロップ回路から構成できる。この場合、n+m本のバスラインに対して、フリップフロップ回路は、 $\log_2(n+m)$ 個必要となる。

【0016】図2は、図1のバススクランブル回路の構成の一例を示すものである。但し、図2では、説明を簡単にするため、バスライン50が2ビットのデータバスから構成されているものと仮定している。

【0017】CPU10の入出力端子I/O・0は、バススクランブル回路11のトランジスタT00を経由してデータバスBD0に接続されると共に、バススクランブル回路11のトランジスタT01を経由してデータバスBD1に接続される。また、CPU10の入出力端子I/O・1は、バススクランブル回路11のトランジスタT10を経由してデータバスBD1に接続されると共に、バススクランブル回路11のトランジスタT11を経由してデータバスBD0に接続される。

【0018】RAM20の入出力端子I/O・0は、バススクランブル回路21のトランジスタT00を経由してデータバスBD0に接続されると共に、バススクランブル回路21のトランジスタT01を経由してデータバスBD1に接続される。また、RAM20の入出力端子I/O・1は、バススクランブル回路21のトランジスタT10を経由してデータバスBD1に接続されると共に、バススクランブル回路21のトランジスタT11を経由してデータバスBD0に接続される。

【0019】ROM30の入出力端子I/O・0は、バススクランブル回路31のトランジスタT00を経由してデータバスBD0に接続されると共に、バススクランブル回路31のトランジスタT01を経由してデータバ

スBD1に接続される。また、ROM30の入出力端子I/O・1は、バススクランブル回路31のトランジスタT10を経由してデータバスBD1に接続されると共に、バススクランブル回路31のトランジスタT11を経由してデータバスBD0に接続される。

【0020】E² PROM40の入出力端子I/O・0は、バススクランブル回路41のトランジスタT00を経由してデータバスBD0に接続されると共に、バススクランブル回路41のトランジスタT01を経由してデータバスBD1に接続される。また、E² PROM40の入出力端子I/O・1は、バススクランブル回路41のトランジスタT10を経由してデータバスBD1に接続されると共に、バススクランブル回路41のトランジスタT11を経由してデータバスBD0に接続される。

【0021】各バススクランブル回路11、21、31、41のトランジスタT00、T10のゲートには、タイミング制御信号φが入力され、各バススクランブル回路11、21、31、41のトランジスタT01、T11のゲートには、タイミング制御信号φが入力される。

【0022】このような構成によれば、例えば、CPU10からRAM20にデータを転送する場合を考えると、CPU10の入出力端子I/O・0から出力されるデータは、バスラインBD0を経由してRAM20の入出力端子I/O・0に到る経路とバスラインBD1を経由してRAM20の入出力端子I/O・0に到る経路の2通りの経路のうちのいずれも取り得ることがわかる。CPU10の入出力端子I/O・1から出力されるデータについても、同様である。

【0023】つまり、タイミング制御信号φ、φのレベルを適当な時期に切り替えることにより、例えば、CPU10の入出力端子I/O・0から出力されるデータは、バスラインBD0を経由してRAM20の入出力端子I/O・0に導かれたり、又はバスラインBD1を経由してRAM20の入出力端子I/O・0に導かれたりすることになる。

【0024】このように、本発明によれば、バススクランブル回路により、データバスBD0、BD1に出力されるデータの意味（又は種類）を時々刻々と変化させることができるため、悪意のアタッカーがIC内を繰り返して解析しても、各バスラインのデータの意味（又は種類）を特定することができず、ICのセキュリティが完璧となる。

【0025】なお、タイミング制御信号φ、φのレベルの切り替え（データ経路の切り替え）は、例えば、特定のブロック（例えば、CPU）の特定の入出力端子I/O・jから出力されるデータに基づいて行うことができる。また、各ブロック間でデータの意味を取り違えないように、タイミング制御信号φ、φのレベルの切り替えは、各ブロック間でのデータの授受が完了した後に

行われる。

【0026】当然に、データ送信側のブロックのバススクランブル回路におけるタイミング制御信号 ϕ 、 ϕ のレベルの切り替え時期とデータ受信側のブロックのバススクランブル回路におけるタイミング制御信号 ϕ 、 ϕ のレベルの切り替え時期は、データの転送時間を考慮すれば、データの転送時間分だけずれることになる。

【0027】タイミング制御信号 ϕ 、 ϕ のレベルの切り替え周期は、例えば、CPUが生成するクロックCLKの周期よりも十分に長くするのがよい。切り替え周期がクロックCLKの周期と同程度に短くなると、データの誤認識の発生する確率が高くなるからである。タイミング制御信号 ϕ 、 ϕ のレベルの切り替え周期は、定期的であっても、ランダムであってもよい。

【0028】図4は、本発明の原理を簡単に示すものである。例えば、CPUから出力されるアドレスがnビット、データがmビットであると仮定すると、バスライン1本で1ビットのデータ転送が可能であるから、アドレスバスとデータバスを合計した本数は、n+m本とな

る。但し、本発明では、上述のように、各バスラインに出力されるアドレス及びデータは、時々刻々と変化するため、n+m本の各バスラインの意味(種類)は特定されない。

【0029】本例では、仮に、n+m本のバスラインにそれぞれ符号BA0~BA_n、BD0~BD_mを付すことにする。この場合、n+mビットの各データの信号経路の組み合わせは、n+mの階乗だけ存在する。よって、バススクランブル回路により、このn+mの階乗だけ存在する信号経路を一定周期で又はランダムに変えてやれば、悪意のあるアタッカーにICの内部が解析されることはない。

【0030】表1は、CPUからアドレス2ビット、データ2ビットが出力されると仮定した場合において、アドレス及びデータの信号経路の組み合わせを全て羅列したものである。

【0031】

【表1】

アドレス2ビット、データ2ビットの場合→24通り

バスライン	データ									
BA0	A0	A0	A0	A0	A0	A0	A1	A1	A1	A1
BA1	A1	A1	D0	D0	D1	D1	A0	A0	D0	D1
BD0	D0	D1	A1	D1	A1	D0	D0	D1	A0	D0
BD1	D1	D0	D1	A1	D0	A1	D1	D0	D1	A0
バスライン	データ									
BA0	D0	D0	D0	D0	D0	D0	D1	D1	D1	D1
BA1	A0	A0	A1	A1	D1	D1	A0	A0	A1	D0
BD0	D1	A1	D1	A0	A0	A1	D0	A1	D0	A0
BD1	A1	D1	A0	D1	A1	A0	A1	D0	A0	D0

【0032】つまり、アドレス及びデータの合計は4ビット、バスラインの数は4本であるから、4の階乗、即ち、24通りの信号経路の組み合わせが考えられる。なお、アドレス及びデータの順序は、送信側のCPUのバススクランブル回路によりランダムに変えられた後にバスラインに出力されるが、当然に、受信側のメモリのバススクランブル回路により正しい順序に戻されてメモリに与えられることになる。

【0033】

【発明の効果】以上、説明したように、本発明のバススクランブル回路によれば、アドレス及びデータの順序を送信ブロック側でランダムに変えた後、バスラインに出力し、かつ、受信ブロック側で正しい順序に戻すような構成とし、アドレス及びデータの転送経路を時々刻々と変化させるようにしている。つまり、各バスラインに出力されるデータの意味(又は種類)が特定されないため、悪意のあるアタッカーがICの内部を繰り返し解析しても、アドレス及びデータを特定できず、完璧なセキュリティシステムを提供することができる。

【図面の簡単な説明】

【図1】本発明のバススクランブル回路を有するICの構成の一例を示す図。

【図2】バススクランブル回路の構成の一例を示す図。

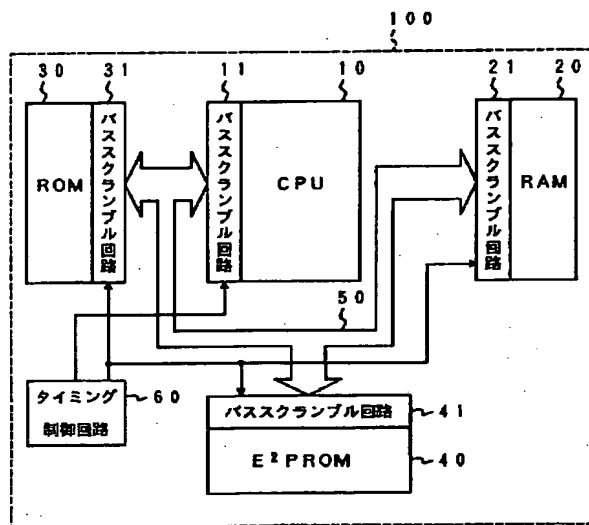
【図3】タイミング制御回路を構成するフリップフロップ回路を示す図。

【図4】本発明の原理を示す図。

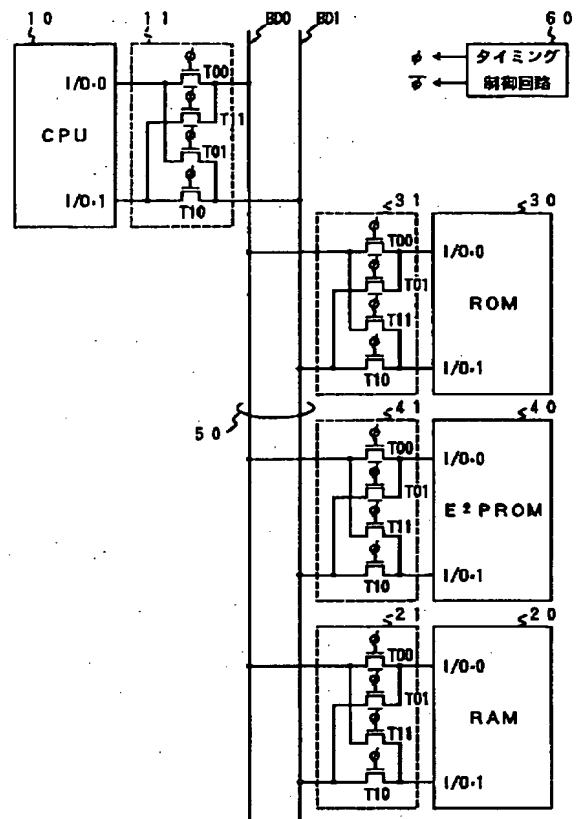
【符号の説明】

10 : CPU、
 11, 21, 31, 41 : バススクランブル回路、
 20 : RAM、
 30 : ROM、
 40 : E² PROM、
 50 : バスライン、
 60 : タイミング制御回路。

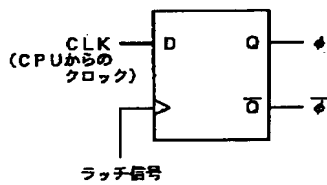
【図1】



【図2】



【図3】



【図4】

